Circuits and Systems, 2016, 7, 1943-1953
Published Online June 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.78169

Efficient Routing Protocol Based on Security for Wireless Sensor Networks

S. Nandhakumar[1], Dr. N. Malmurugan[2]

[1]Department of Computer Science Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, India
[2]Department of Electronics and Communication Engineering, Mahendra College of Engineering, Salem, India
Email: ps.nanthakumar@gmail.com, n.malmurugan@gmail.com

Received 20 February 2016; accepted 15 March 2016; published 28 June 2016

Abstract

Nowadays, the major part and most standard networks usually used in several applications are Wireless Sensor Networks (WSNs). It consists of different nodes which communicate each other for data transmission. There is no access point to control the nodes in the network. This makes the network to undergo severe attacks from both passive and active devices. Due to this attack, the network undergoes downgrade performance. To overcome these attacks, security based routing protocol is proposed with the security based wormhole detection scheme. This scheme comprises of two phases. In this approach, the detection of wormhole attacks is deployed for having correct balance between safe route and stability. Also, to ensure packets integrity cryptographic scheme is used as well as authenticity while travelling from source to destination nodes. By extensive simulation, the proposed scheme achieves enhanced performance of packet delivery ratio, end to end delay, throughput and overhead than the existing schemes.

Keywords

WSNS, Throughput, Integrated Cryptography Scheme, Delivery Ratio, Packet Loss, Authentication, Data Integrity, Communication Overhead and End to End Delay

1. Introduction

1.1. Wireless Sensor Networks (WSNs)

The Wireless Sensor Networks contain several mobile nodes which form communication among themselves without a fixed infrastructure. It is frequently used in special situations such as in emergency operations on natural or manmade disasters, rescue activities, battle fields or seminar halls particularly in areas where no infrastructure fixed or destroyed such infrastructure. A node may either function as an end node or between source

How to cite this paper: Nandhakumar, S. and Malmurugan, Dr.N. (2016) Efficient Routing Protocol Based on Security for Wireless Sensor Networks. *Circuits and Systems*, **7**, 1943-1953. http://dx.doi.org/10.4236/cs.2016.78169

and destination nodes as a router forwarding the data packets. So there is a need of effective routing mechanism which needs to maintain acceptable service quality during communication between nodes.

As discussed in [1], recently chip technology development makes the handheld devices have faster processing power and consume less energy. There are wired and wireless significant differences in the network. The wired networks have relatively high topology and bandwidth which varieties irregularly. In dissimilarity, wireless networks have limited bandwidth resource, and their nodes have high mobility. Furthermore, it have high rate of link breakage, which leads to high partitioning rate of the network. So, the classic Bellman-Ford based routing protocols incur too much overhead and take long time to converge and not suitable for ad hoc network. In WSNs, the messages may be forwarded through multiple hops due to the range limitation of radio transmission in each mobile computer. Discovery paths, *i.e.*, routing is an essential mechanism to support the multiple hop radio transmissions.

Also, the node mobility and limited communication resources make routing very difficult in WSNs. The existing path can break by the causes of regular topology changes by the mobility. The frequent changes of topology have to be adapted by the routing protocol quickly and need to find out new paths efficiently. On the other hand, in WSNs, the limited resources of bandwidth and the power are very challenging for rapid reworking. More importantly, resource constraints in WSNs require a routing protocol to fairly distribute routing tasks among the mobile hosts. As a result, power energy quickly may reduce by the heavily loaded hosts, which will lead to the failure and networks partitions of the application sessions. Obviously, here is a claim for a new routing strategy to solve these issues.

As an alternative to single shortest path routing, the multipath routing is proposed in the network to distribute load and alleviate congestion. In multipath routing, traffic certain to a destination is split across multiple paths to that destination. In other words, multiple "good" paths instead of a single "best" path for routing is consider in the multipath routing. It establishes multiple paths between pairs of begin and end of the communication network and thus requires more hosts to be responsible for the routing tasks.

1.2. Wormhole Attacks in WSNs

In the network, the attacker obtains the packets at one location and passageways packets to another location. This is carried out between two colluding attackers as a wormhole. This process is established through a wired or single long-range wireless link between the two colluding attackers. As well as, the attacker can even create packet with wormhole by the nature of radio channel broadcast for not to addressed to them.

In **Figure 1**, the malicious nodes (P and Q) are encapsulating the packet data's and the lengths of rout are falsified. The route discovery is initiates the route to form from source to destination as new route.

In this case of {**P** → **P** → **Q** → **R** → Q}, through the existing route the Q will pass and encapsulates the request of route, if P receives a Route Request from S. When Q receives request for D then it show the travel {**S** → **P** → **Q** → **D**} and the packet header will update by neither P nor Q. After route discovery, the unequal route length from s is defined in the destination that it has two routes *i.e.* one is 4 and another is 3.

If the route reply is back to P from Q tunnels then, S would incorrectly deliberate the path to D through P and it is well than the path from R to D. Thus, the intermediate nodes are prevented from appropriate increment of

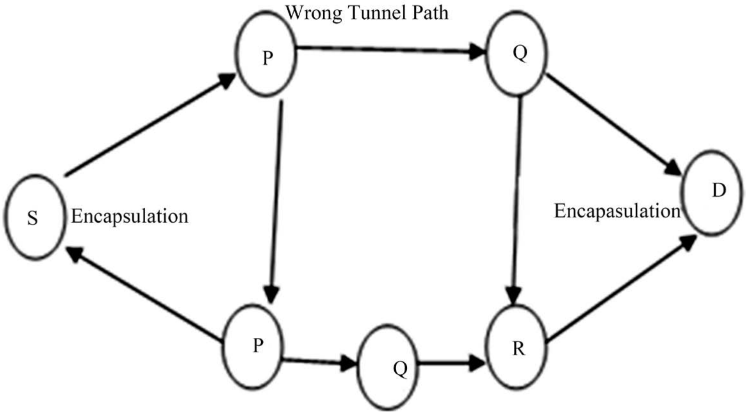


Figure 1. Wormhole attack.

the metric used to measure path lengths by using tunneling. As well as, if the wormhole is properly used for efficient packets relaying then no harm will be. In the network, the attacker is placed in an influential position when associated with the other nodes for the network security purposes.

The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the packet transmission of the nodes hear directly from some node consider themselves to be in range of that node. **Figure 2** shows the wormhole attack process. In network, an attacker obtains packets at one point, tunnels and replays in another point.

Due to the nature of wireless transmission, the attacker can generate a wormhole for not to address them, since it eavesdrops to the attacker plotting at the opposite end of the wormhole. The communication link of private is shared between the two malicious nodes. The wormhole can eaves drop the traffic, unkindly packets drop, and attain man-in-the-middle attacks against the network protocols.

The paper is organized as follows. The section 1 describes with overview of WSNs and Wormhole attacks. The section 2 deals with the literature survey. The section 3 is devoted for the implementation of proposed algorithm. The section 4 describes the performance analysis and the last section 5 concludes the work.

2. Related Work

In this section, the survey related to the secure routing in the wireless network is discussed. T. Sakthivel and R. M. Chandrasekaran [2] proposed Path Tracing (PT) algorithm is used to detect and prevent the wormhole attack as an extension of DSR protocol. The discovery of DSR route process is carried out with the process of PT algorithm in a path on each node. It computes per hop distance based on the value of RTT and using frequency appearance count the wormhole link is estimated. The normal link participates lesser than the wormhole link during the process of routing. By using link frequent appearance count the link of wormhole is detected.

Shalini Jain and Dr. Satbir Jain [3] presented the novel trust-based scheme for identifying and isolating nodes which produce a wormhole without engaging any cryptographic in the network. It is derived that trust levels in neighbouring nodes is based on their authenticity of the routing protocol execution. This is used for the routing decisions for the avoidances of communication through wormholes.

S. Madhavi and K. Duraiswamy [4] proposed a new methodology to detect and prevent the wormhole attack during the route discovery process. In a reactive routing protocol, whenever the node initiates the communica-

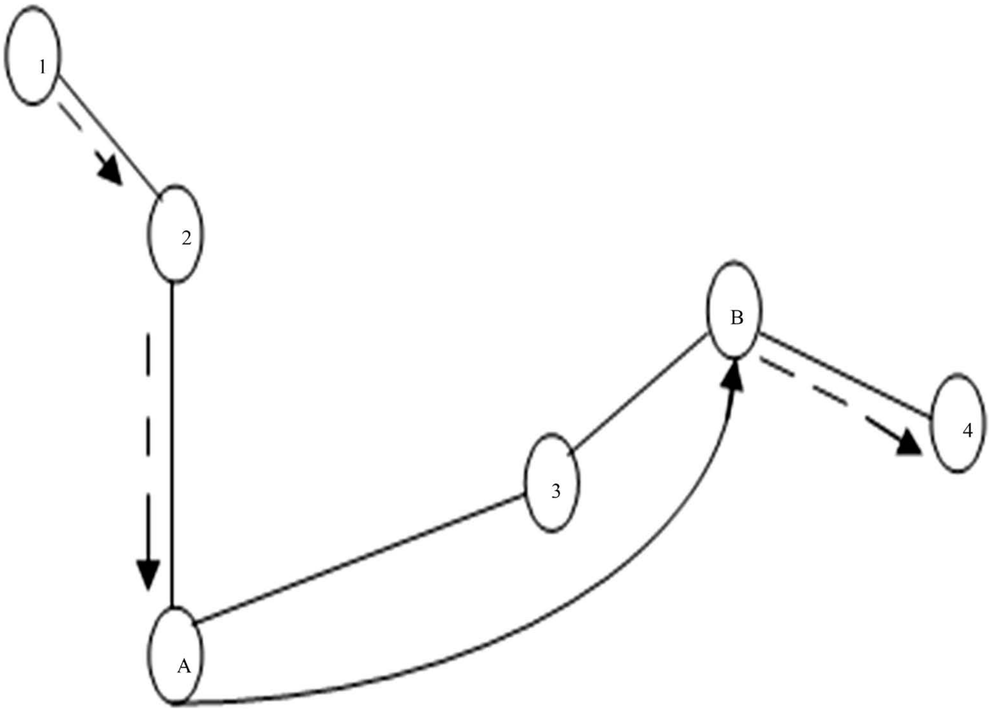


Figure 2. A wormhole attack performed by malicious nodes A and B.

tion process it checks the table of routing. It will send the packet only if the entry is available for the node of destination otherwise it finds the path through Route Request (RREQ) and Route Reply (RREP) control packets. Source sends the selection packet to the participants to inform valid path for this session. The proposed work has been designed to use hello packets to the calculate decision count at every intermediate node to identify the malicious.

Revathi *et al.* [5] addressed few related works concerned with wormhole attacks. For the detection of wormholes the graph theoretic approach based on adjacency matrix is proposed in mobile ad hoc network. Until, the complexity of computation in a mobile node not increasing which is resource constrained, this approach is beneficial.

Xu Su and Rajendra V. Boppana [6] proposed NEighbor Verification by Overhearing (NEVO), in which nodes passively monitor (overhear) the broadcast type packets forwarding by their neighbours and use the send and overhear times of transmissions of these packets for the moderate of the wormhole attacks. The synchronized clocks, special hardware support, or any special capability are not required in NEVO. It can detect almost all instances of wormhole attacks and is virtually liberated of the routing protocol used.

Issa Khalil *et al.* [7] proposed a protocol called MOBIWORP in mobile networks of multi-hop ad hoc and sensor for mitigating the wormhole attack. It incorporates two protocols SMP and CAP-CV for differing degrees of functionality afforded to a mobile node. They also proposed local and global isolation protocols that will deactivate the ability of the malicious nodes from initiation of further attacks after detection, either in new or current location. The MOBIWORP effects are demonstrated under various network conditions and mobility patterns using simulations.

S. Sharmila and G. Umamaheswari [8] explored the transmission time based scheme to detect the wormhole attack using AODV routing protocol. The transmission time of the route request and reply in the routing path is calculated between all successive nodes. The additional control packet is transmitted between the suspected wormholes for further confirmation. The proposed work is able to detect the both the hidden attack and exposed attack.

Pallavi Sharma *et al.* [9] presented a mechanism which is helpful for detection and defend against the wormhole attack in ad hoc network is ”multipath hop counting analysis” (MHA) which tolerant all route request at destination node with in a fixed time period called time to live (TTL) period. In proposed solution, if sender wants to send the data to destination, then secure path is required to create between sender and receiver with the help of multipath hop count analysis and verification of digital signature. The malicious node presence in between the path will be identified because of the malicious node does not have its own legal digital signature.

Amol A. Bhosle *et al.* [10] presented a watchdog mechanism and time of flight to identify and overcome the attacks of wormhole and black hole attack. Also, it improves the data security in mobile ad-hoc network. This method is used in the network for the detection of black hole attack and then provides a new route to this node. In a wormhole attack, intruders tunnel the data from end to end of the network. The leading distant network nodes are make to trust that they are neighbours and making them communicate through the wormhole link.

Rakesh *et al.* [11] proposed a novel cross layer intrusion detection architecture towards determining the malicious nodes and different types of DoS attacks by manipulating the available data across dissimilar layers of protocol stack in order to improve the accuracy of detection. They have used cooperative anomaly intrusion detection with data mining technique to enhance the proposed architecture. It is implemented fixed width clustering algorithm for efficient detection of the anomalies in the WSNS traffic and also generated different types of attacks in the network.

Sandeep *et al.* [12] reviewed the literature available on cross-layer design, and categorized the survey on different features like definition, motivation, various cross layer proposals and their categories, evaluating factor and various open challenges in this domain. When the channel is wireless then authentication of the wireless terminal is a serious issue which can be solved by proper authentication of the wireless terminal. Physical layer authentication in which the channel probing or channel estimation is used when integrated with the cross-layer design can enhance the security of the network.

Ravneet Kaur [13] dealt with cross layer based miss detection ratio under variable rate for intrusion detection in WLAN. Based on the decision of the combination of weighted value layer, cross layer based intrusions detected. The decision on multilayer will reduce false positive rate. The obtained results from using physical and MAC layer is being compared with the traditional techniques.

K. Srinivas, A. A. Chari [14] proposed the cross layered model of congestion detection of a control mechanism which contains Zone level Egress Regularization Algorithm [ZERA], energy efficient congestion detection and Zone level Congestion Evaluation Algorithm [ZCEA], which is a hierarchical cross layer based control model and congestion detection approach. By experimental results the proposed approach achieved the better resource consumption and energy efficiency in congestion control and detection.

V. Thilagavathe and Dr. K. Duraiswamy [15] proposed the cross-layer based technique to overcome congestion that occurs in MAC and transport layer in WSNS. The proposed system was functional over an Ad hoc on demand Multipath Reliable and Energy Aware QoS Routing Protocol (AOMP-REQR). The procedure of additive increase and multiplicative decrease (AIMD) was applied for rate based congestion control of transport layer protocol. The transmission is established by the congestion free route without execution of rate control only if source receives the status of congestion information from both MAC and transport layer simultaneously for the same route.

Shitalkumar Jain *et al.* [16] reviewed that signal strength based measurements used to improve such packet losses and not necessary to retransmit the packets. So, the node and link based signal strength can be measured. A node avoids congestion by choosing alternate path when there is weak signal strength.

Rajkumar, G. *et al.* [17] proposed congestion aware multi path routing protocol for the losses reduction of congestion detection. The congestion control technique is followed which proactively notices the congestion level of link and node and also performs congestion control using the fault-tolerant multiple paths. The approach of congestion detection is based on buffer. On reception of a data packet, each intermediate node observers its current size of buffer and estimates the running average value using the expression of exponential weighted moving average. If the predefined threshold is lesser than the average value, then the congestion is detected. Whenever the source node obtains the packet of the congestion control sent by the congested node, it executes the congestion control approach. This proposed scheme permits more nodes to recover a dropped packet.

Kazuya *et al.* [18] analysed a routing protocol that reduces the network congestion by using multi-agents for a Mobile Ad hoc NETwork (MANET). MANET is a multi-hop wireless network with the components such as PDA, PC and mobile phones are mobile. The components can communicate without going over and done with a server with each other. The two kinds of agents are engaged in routing. One is Routing Agent gathers information about network congestion with the link failure. The other is a Message Agent which uses the data to get to their destination nodes.

3. Proposed Work—Security Based Routing Protocol (SRP)

The future wormhole attack detection mechanism is includes with the security based routing protocol in two phases. In this approach, the worm hole attack is detected is inaccessible using alternate path discovery. It is based on mobility and the design is carried out in protocol layers. The data integrity and authenticity can be provided using IRSA algorithm. By this reliable protocol of routing is implemented for defending against the attacks of wormhole.

Reliable Routing Protocol for Defending Against Wormhole Attacks

1) Source node S sends a message to Destination node D in order to create a shared secret session key for the communication link using IRSA algorithm.
2) If Source node receives a reply message from Destination node within the Network Cross Time (N_{CT}).
3) Then, it is the maximum expected time in milliseconds waiting for receiving of a Route Reply (RREP) after sending of Route Request (RREQ). Then
4) Source and Destination node D implements the Improved Reverse Shamir Adleman (IRSA) algorithm.
5) S sends an encrypted with the secure session key message SSK-ERP to the destination using the Advance Encryption Standard (AES) and records the current time t_{erp}.
6) D decrypts the SSK-ERP and includes its destination ID number. It encrypts the SSK-ERP using AES and send back to the Source node.
7) If Source node S does not receive the SSK-ERP within the Network Cross Time. Then,
8) S considers the route R is attacked by wormhole attack.
9) S deletes the route R from its routing table.
10) Source node S informs the misbeh-ward with the next hop node and exit.
11) Else, stores the receiving time $t_{erp.}$
12) S determines the Original Traversal Time (O_{TT}). The time from sending of RREQ until the receiving of a RREP.
13) If the O_{TT} is less than or equal to Original Threshold Traversal Time (T_{OTT}). Then estimate as the combination of Probability of misbehaviour ratio and Packet Loss Rate.

14) The route is considered as a Safe Route and exit.
15) Else, S considers the route R is attacked by wormhole attack and continues with step 7 until it reach safe route.
16) End if the probability of Misbehavior Ratio (MR) and the Packet Loss Ratio (PLR) is defined as

$$P_{LT}\left(t_1,t_2\right)=\frac{\int_{t_1}^{t_2} 1_{\{G(t)=D_l\}}\mathrm{d}K\left(t\right)}{\int_{t_1}^{t_2}\mathrm{d}K\left(t\right)} \tag{1}$$

$$P_{MR}=\frac{Max\left(0,P_{LT}\right)\times P_{BP}\times P_{LACK}}{P_{TR}} \tag{2}$$

where, $K(t)$ is for the user packets arrival process. Here, the number of user packets sent in $[t_1, t_2]$ is represents by the denominator and the numerator represents the number of lost user Packets. P_{BP} represent the probability of bad packet occurrence, P_{LACK} as the probability of acknowledgement packet lost due to link failure and P_{TR} as a total number of packets received. The procedure of the proposed system is given below. According to the steps the execution of the proposed approach is carried out in the network.

***Encryption and Decryption*:**

Encryption:

- Original plain text (a block value) = F ... F < N.
- Chiper text = C ... C = (F^E) mod N

C = F^e mod N

Send encrypted data X and session.

- Y = Ksim(F), T = Kpub(Y),
- Y = Kpri (T), F = Ksim(Y)

Get private key from file

- Initialize the data for decryption with private key and with session key.

Decryption:

- Chiper text = C;
- Plain text = F;
- F = C^d mod N

(or)

- By Using CRT

M1 = C^{dP} mod P

M2 = C^{dQ} mod Q

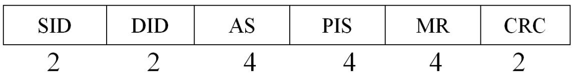
H = (M1 − M2) inv Q mod P

Y = M2 + (Q * H)

where, KD referred as key derivation function; EN as an encryption function; DE as a decryption function; MA as a message authentication code.

***Proposed Packet Format*:**

As shown in **Figure 3** the proposed packet format is carried out. Here the ID of the source and destination node (S ID and D ID) carries 2 bytes. Third one is authentication status of the node. The authentication status (AS) induces the whether the transmission of packets are travelled through authenticated route. The packet integrity status (PIS) is indicated in the fourth field. It determines how much transmission of the genuine packets is carried out between source and destination node. It also determines whether packet contains authorized information. In fifth, the misbehaving rate (MR) is allotted to ensure detection of misbehaviors. The last filed CRC *i.e.* Cyclic Redundancy Check for error correction and detection in packet while route maintenance process.



SID	DID	AS	PIS	MR	CRC
2	2	4	4	4	2

Figure 3. Proposed packet format.

4. Performance Analysis

In this section, the simulation of the proposed work is carried out by using Network Simulator tool with version 2.34. The performances of the proposed system and the comparison analysis are presented. In this simulation tool, the C++ language is back end language and tool command language (tcl) is front end language. The basic advantage of this tool is more updating compare to Glomosim, JIST and Qualnet etc. In our simulation, 100 mobile nodes move in a 1000 meter × 1000 meter square region for 100 seconds simulation time. The transmission range of 200 meters is same for all nodes. The simulated traffic is Constant Bit Rate (CBR) and Poisson traffic.

The simulation results are presented in the next part. Here, the proposed SRP is compared with the FTD [18] and SZRP [19] in presence of congestion environment. The performances are evaluated according to the following metrics.

Packet Delivery Ratio: This factor indicates that ratio of number of packets received to the number of packets sent.

Misbehavior Ratio: The number of routing control packets are affected by the wormhole attacks.

End to end Delay: The delay in the packet from source to destination during the transmission.

Overhead: It is the ratio of number of control packets received to the total number of packets being sent.

The simulation settings and parameters are summarized in **Table 1**.

Figure 4 shows the results of packet delivery ratio for varying from 10 to 50 secs of the simulation time.

Table 1. Simulation settings and parameters.

No. of Nodes	200
Area Size	1200 × 1200
Mac	802.11
Radio Range	250 m
Simulation Time	70 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	Dynamic Source Routing
Pause time	5 msec

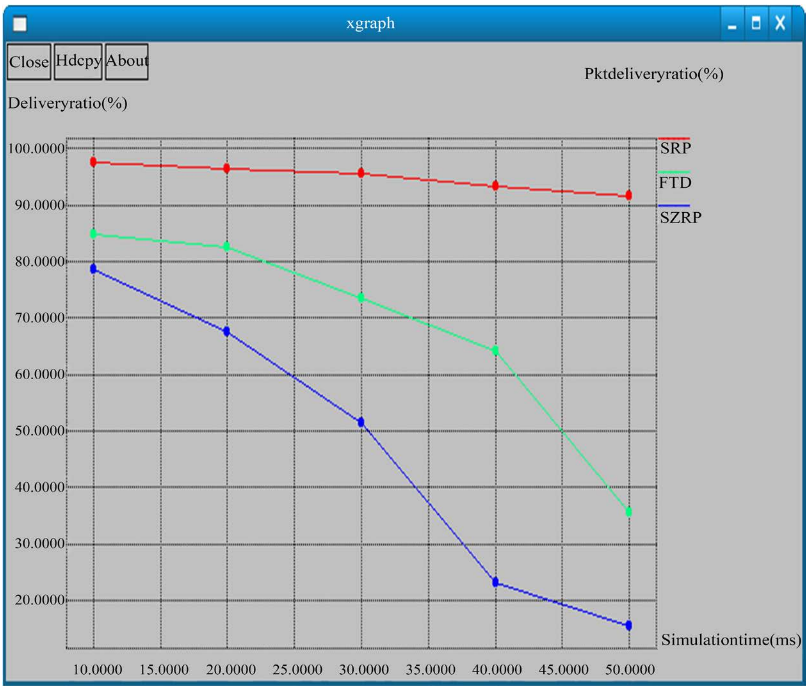


Figure 4. Simulation time vs delivery ratio.

From the results, SRP scheme has higher delivery ratio than the FTD and SZRP because of integrated cryptography scheme.

Figure 5 presents the comparison of communication overhead. It is clearly shown that the overhead of SRP has low overhead than FTD and SZRP.

Figure 6 shows the results of Mobility Vs End to end delay. From the results, we can see that delay of SRP is

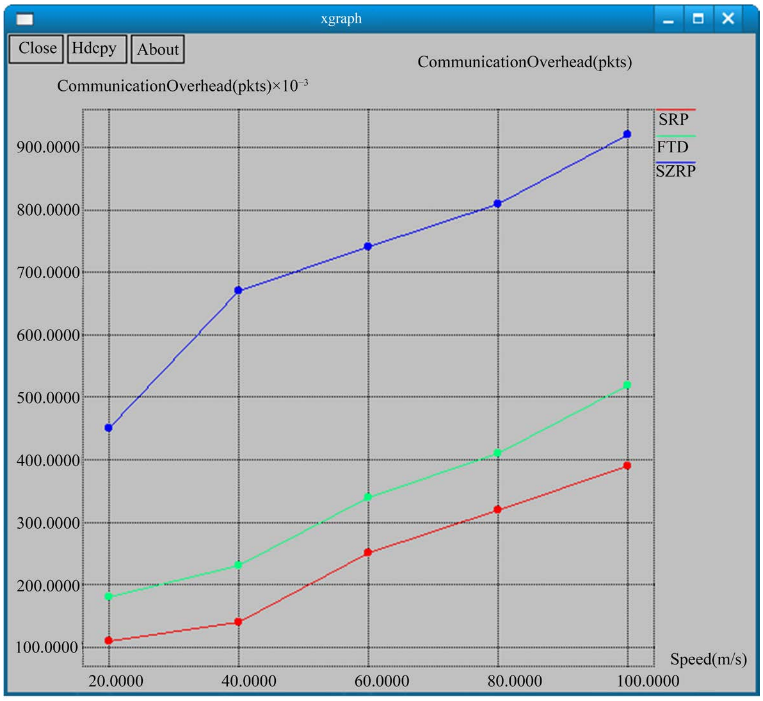


Figure 5. Speed vs communication overhead.

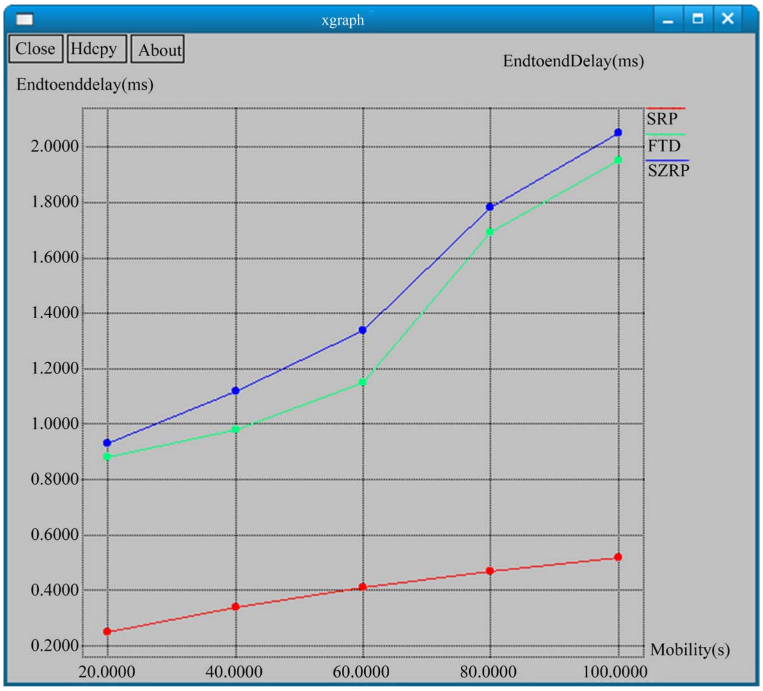


Figure 6. Mobility vs end to end delay.

lower than FTD and SZRP while varying the mobility from 10 to 100 ms.

Figure 7 presents the comparison of authentication rate while varying the simulation time from 10 to 50 secs. It is clearly shown that the authentication rate of SRP has relatively high than FTD and SZRP.

Figure 8 presents the comparison of throughput while varying the number of nodes from 10 to 200. It is clearly shown that the throughput of SRP has relatively high than FTD and SZRP.

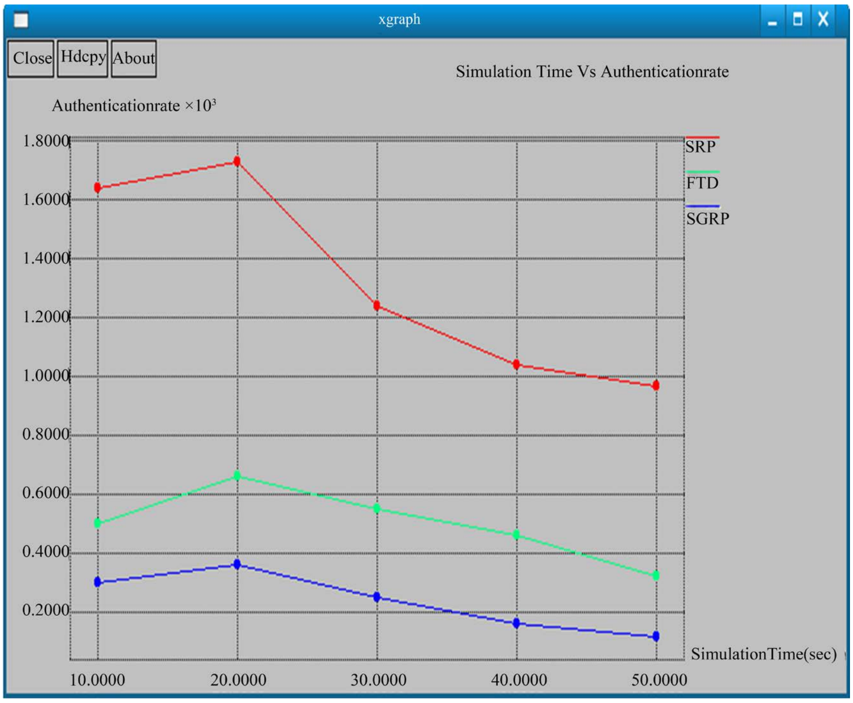


Figure 7. Simulation time vs authentication rate.

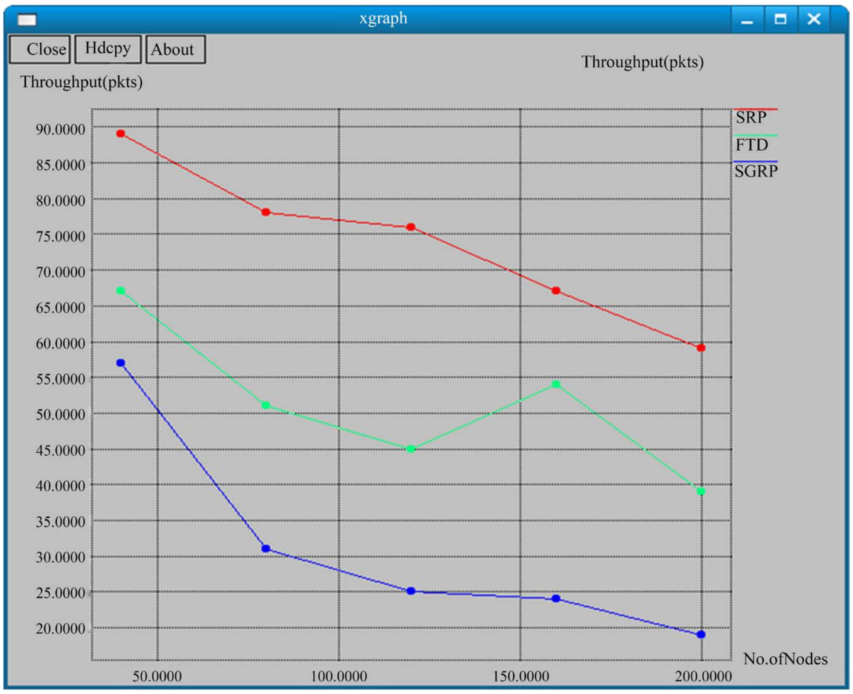


Figure 8. No. of nodes vs throughput.

5. Conclusion

Due to the presence of attacks in WSNS, the nodes are easily impersonated by wormhole attacks. To overcome the issue of wormhole attacks, we propose to design the security based routing protocol for ad hoc networks. We achieve the detection of wormhole misbehavior using threshold value of network cross time. The integrated cryptography scheme is developed to achieve the data integrity. The proposed work SRP achieves the better packet delivery ratio, low delay and overhead than the existing schemes while varying the mobility, time, throughput speed and number of nodes. In future, we extend this work to energy consumption model and authentication approach.

References

[1] Devi, B.A.S.R., Narasimha, G. and Murthy, J.V.R. (2013) Secure Zone Based Routing Protocol for Mobile Ad Hoc Networks. *International Conference on Automation*, *Computing*, *Communication*, *Control and Compressed Sensing*, 839-846

[2] Sakthivel, T. and Chandrasekaran, R.M. (2012) Detection and Prevention of Wormhole Attacks in MANETs Using Path Tracing Approach. *European Journal of Scientific Research*, **76**, 240-252.

[3] Jain, S. and Jain, S. (2010) Detection and Prevention of Wormhole Attack in Mobile Adhoc Networks. *International Journal of Computer Theory and Engineering*, **2**, 78-86.

[4] Madhavi, S. and Duraiswamy, K. (2012) WAS-DP: Wormhole Attack in SAODV-Detection and Prevention. *European Journal of Scientific Research*, **77**, 560-569.

[5] Venkataraman, R., Pushpalatha, M., Rama Rao, T. and Khemka, R. (2009) A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc Networks. *International Journal of Recent Trends in Engineering*, **1**, 220-222.

[6] Su, X. and Boppana, R.V. (2008) Mitigating Wormhole Attacks using Passive Monitoring in Mobile Ad Hoc Networks. *IEEE Global Telecommunications Conference*, 1-5.

[7] Khalil, I., Bagchi, S. and Shroff, N.B. (2008) MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks. *Ad Hoc Networks*, **6**, 344-362. http://dx.doi.org/10.1016/j.adhoc.2007.02.001

[8] Sharmila, S. and Umamaheswari, G. (2012) Transmission Time Based Detection of Wormhole Attack in Wireless Sensor Networks. Special Issue of International Journal of Computer Applications (0975-8887) on Information Processing and Remote Computing—IPRC, August 2012.

[9] Sharma, P. and Trivedi, A. (2011) Prevention of Wormhole Attack in Ad-Hoc Network. Special Issue of International Journal of Computer Applications (0975-8887) on Electronics, Information and Communication Engineering—ICEICE No.5, December 2011, 13-17.

[10] Bhosle, A.A., Thosar, T.P. and Mehatre, S. (2012) Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET. *International Journal of Computer Science*, *Engineering and Applications* (*IJCSEA*), **2**, 45-54. http://dx.doi.org/10.5121/ijcsea.2012.2105

[11] Shrestha, R., Han, K.-H., Choi, D.-Y. and Han, S.-J. (2010) A Novel Cross Layer Intrusion Detection System in MANET. 2010 24*th IEEE International Conference on Advanced Information Networking and Applications*, Perth, WA, 20-23 April 2010, 647-654.

[12] Sharma, S., Mishra, R. and Singh, K. (2012) Current Trends and Future Aspects in Cross Layer Design for the Wireless Networks. *Computer Science & Information Technology* (*CS & IT*), 283-296.

[13] Kaur, R. (2011) Cross Layer Based Miss Detection Ratio under Variable Rate for Intrusion Detection in WLAN. *International Journal of Computer Engineering Research*, **2**, 75-81.

[14] Srinivas, K. and Chari, A.A. (2012) ECDC: Energy Efficient Cross Layered Congestion Detection and Control Routing Protocol. *International Journal of Soft Computing and Engineering* (*IJSCE*), **2**, 316-322.

[15] Thilagavathe, V. and Duraiswamy, K. (2011) Cross Layer Based Congestion Control Technique for Reliable and Energy Aware Routing in MANET. *International Journal of Computer Applications*, **36**, 1-6.

[16] Jain, S. and Usturge, S.I. (2011) Signal Strength Based Congestion Control in MANET. *Advances in Physics Theories and Applications*, **1**, 26-36.

[17] Rajkumar, G. and Duraiswamy, K. (2012) A Fault Tolerant Congestion Aware Routing Protocol for Mobile Ad hoc Networks. *Journal of Computer Science*, **8**, 673-680. http://dx.doi.org/10.3844/jcssp.2012.673.680

[18] Nishimura, K. and Takahashi, K. (2007) A Multi-Agent Routing Protocol with Congestion Control for MANET. 21*st European Conference on Modelling and Simulation*, Prague, 4-6 June 2007, 1-6.

http://dx.doi.org/10.7148/2007-0164

[19] Dong, D.Z., Li, M., Liu, Y.H., Li, X.-Y. and Liao, X.K. Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks. *IEEE/ACM Transactions on Networking*, **19**, 1787-1796.